UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,238	04/18/2001	Peter T. Dinsmore	NAI1P090/00.176.01	6439

28875 7590 08/09/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/836,238	DINSMORE ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 22 December 2004 has been noted and made of record.

2. Claims 1-30 have been presented for examination.

3. Claims 4, 10, 15, and 23 have been cancelled as per Applicant's request.

Response to Arguments

4. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as the definition of a power set or a reusable power set, are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

5. Applicant's arguments with respect to claims 1-3, 5-9, 11-14, 16-22, and 24-30 have been considered but are moot in view of the new ground(s) of rejection.

6. See further rejections that follow.

Claim Rejections

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-3, 5-9, 11-14, 16-22, and 24-30 are rejected under 35 U.S.C. 102(b) based upon a public use or sale of the invention. As evidenced by **Key Management for Large Dynamic Groups: One-way Function Trees and Amortized Initialization**, from the IRTF SMUG Meeting on 15 March 1999, which outlines security and key management for very large, dynamic multi-party applications. On page/slide 4, the formation of sub groups and member eviction is first touched upon. On page/slide 5, the introduction of re-keying using one-way function trees is brought up as it "scale[s] best to very large groups." On page/slide 10, the features and advantages of one-way function trees is discussed and include things such as key derivation via hashing, scalability, and accommodation of sub-groups. The subgroup updating the leaf key independently is introduced on page/slide 11, which states that the group base key is derived from the system base key using a one-way function.

10. Claims 1, 3, 6-9, 11-14, 17, 19-22, and 24-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over ***Ioulus: A Framework for Scalable Secure Multicasting***, by Suvo Mittra, hereinafter Mittra, in view of U.S. Patent No. 6,606,706 B1 to Li, hereinafter Li, and in further view of **Dynamic Cryptographic Context Management (DCCM), Report #4** by David M. Balenson et al., hereinafter Balenson.

11. As per claims 1, 11, 17, 24, and 25, Mittra discloses associating a subgroup of a group with a leaf node of a hierarchical tree (p. 280, column 2, i.e. "The secure distribution tree is composed of a number of smaller secure multicast "subgroups" arranged in a hierarchy to create a single virtual secure multicast group," wherein the leaf node is drawn to the "group security intermediaries" or "group security agents").

12. Mittra also discloses wherein the leaf node has a leaf key common to the members of the subgroup (p. 280, column 2, i.e. "Moreover, each group has its own subgroup keying material (K_{SGRP} in short) and there is no global K_{GRP}.")

13. Mittra discusses two types of evictions of members from the groups (p. 282, column 2, i.e. "(1) a member wishes to voluntarily leave the subgroup in which case it sends a LEAVE request to the GSA, or (2) the GSA wants to expel a member of the subgroup and sends a notification to that effect to the expelled member").

14. Mittra does not disclose wherein leaf key enables the members of the subgroup to receive an update message for an interior node above the leaf node.

15. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the leaf key enable members of the subgroup to receive an update message from an interior node that is above the leaf node (Li, column 10, lines 5-14, column 11, lines 34-43), since Li states at column 2, lines 12-25 that such a modification would reduce latency incurred by decrypting and re-encrypting data received from and transmitted to each subgroup.

16. Mittra and Li do not disclose wherein said subgroup is a self-repairing group, said self-repairing group being operative to update said leaf key independently;

wherein each of said members of said subgroup is capable of independently updating a shard interior node key.

17. Balenson teaches wherein said subgroup is a self-repairing group, said self-repairing group being operative to update said leaf key independently; wherein each of said members of said subgroup is capable of independently updating a shard interior node key (page 7, **5.2.2 OFT**

Operations, i.e. during group induction, each member establishes an individual group base key known only by the member and the group manager).

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the subgroup be a self-repairing group capable of independently updating the key, since Balenson states at page 8, section **5.3**, that such a modification would require fewer bits to transmit for the re-keying thereby minimizing the number of bits for the broadcast, thus preventing the re-keying operation from becoming a drain on bandwidth.

19. Regarding claim 2, Balenson discloses wherein said evicted member is not a part of said subgroup (page 7, **5.2.2 OFT operations**, *Evicting a member*, i.e. changing the key for sibling members not part of the group).

20. Regarding claim 3, Mittra discloses wherein said evicted member is part of said subgroup (p. 282-283, **Section 6.4 Leaves**).

21. Regarding claims 6 and 19, Balenson discloses wherein key updates are performed using a logical key hierarchy method (page 5, **5. Key Management**, *Heirarchical, tree-based methods)*.

22. Regarding claims 7 and 20, Balenson discloses wherein key updates are performed using a one-way function tree method (pages 5-7, **5.2 One-way Function trees**).

23. Regarding claims 8 and 21, Balenson teaches wherein key updates are performed using a one-way function chain method (pages 5-7, **5.2 One-way Function trees**).

24. Regarding claims 9 and 22, Balenson discloses wherein said hierarchical tree is a binary tree (pages 5-7, **5.2 One-way Function trees**).

25. Regarding claim 12, Mittra discloses wherein said evicting comprises evicting one member of said group (p. 282-283, **Section 6.4 Leaves**).

26. Regarding claim 13, Mittra teaches wherein said evicting comprises evicting more than one member of said group (p. 282-283, **Section 6.4 Leaves**).

27. Regarding claim 14, Mittra discloses wherein said notifying comprises transmitting identities of said at least one evicted member (p. 282-283, **Section 6.4 Leaves**).

28. Regarding claim 26, Balenson discloses wherein said updating of said shared interior node key is carried out in a single step (pages 5-7, **5.2.1 OFT structure**).

29. Regarding claim 27, Balenson teaches wherein said updating of said shared interior node key is not dependent on key distribution messages from a root node that update further node keys descending from said shared interior node key (pages 7-8, **5.2.2 OFT operations**).

30. With regards to claim 28, Balenson discloses wherein said reusable power set uses a power set of said members in said subgroup as a basis for group key updates (pages 7-8, **5.2.2 OFT operations/properties)**.

31. Concerning claim 29, Balenson teaches wherein said reusable power set includes 2^N sets, where N includes the number of said members (pages 7-8, **5.2.2 OFT operations**, i.e. adding a member in a hierarchical tree the set would be based on 2^N).

32. Concerning claim 30, Balenson teaches wherein said reusable power set includes 2^{N-1} sets, where N includes the number of said members (pages 7-8, **5.2.2 OFT operations**, i.e. evicting a member in a hierarchical tree the set would be based on 2^{N-1}).

33. Claims 5, 16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra, Li, and Balenson as applied above, and further in view of U.S. Patent No. 6,240,188 to Dondeti et al., hereinafter Dondeti.

34. Concerning claims 5, 16, and 18, Mittra, Li, and Balenson do not disclose wherein said self-repairing group uses a reusable power set.

35. Dondeti teaches wherein said self-repairing group uses a reusable power set (column 3, line 47 to column 4, line 65).

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the self-repairing group use a reusable power set, since Dondeti states at column 2, lines 7-34 that such a modification would allow users to generate keys when users join

or leave a group while preventing those who have been evicted from colluding with those that remain to view presently encrypted messages.

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

38. The following patents are cited to further show the state of the art with respect to key updates in a distributed system, such as:

United States Patent No. 6,049,878 to Caronni et al., which is cited to show group key management in a multicasting environment.

United States Patent No. 6,275,859 to Wesley et al., which is cited to show tree-based reliable multicast system where sessions are established by repair nodes to authenticate receiver nodes.

United States Patent Application Publication No. 2002/0147906 to Lotspiech et al., which is cited to show broadcast encryption and key revocation of stateless receivers.

39. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

40. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

42. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

43. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100